

TECHNISCHE ANALYSE
W32/{CONFICKER,KIDO,DOWNADUP}



UNIVERSITY OF APPLIED SCIENCES
HAGENBERG

Philipp WINTER
sec08015@fh-hagenberg.at

25. Februar 2009

Inhaltsverzeichnis

1	Grundlegendes	2
1.1	Einleitung	2
1.2	Analysierte Datei	2
1.3	Erstes Auftauchen	3
1.4	Varianten	3
2	Infektion und Weiterverbreitung	4
2.1	Grundlegendes	4
2.2	Die MS08-67 Lücke	5
2.3	Netzwerkfreigaben	5
2.4	Mobile Datenträger	7
3	Aktivität auf infizierten Hosts	7
3.1	Installation	7
3.2	Verschleierung der Existenz	8
3.3	Verhinderung von Gegenmaßnahmen	9
3.4	Nachladen von Payload	11
4	Abwehr und Prävention	12
4.1	Rechtzeitiges Patchen	12
4.2	Sicherheitspolicies	13
4.3	Starke Passwörter	13
5	Fazit	13
6	Anhang	14

1 Grundlegendes

1.1 Einleitung

Dieses Dokument beschreibt die Analyse des Wurms, der gemeinhin unter dem Namen W32 Conficker/Kido/Downadup¹ bekannt ist und unter anderem die MS08-67 [9] Lücke zur Verbreitung ausnützt. Diese Lücke im Windows Server Service betrifft alle derzeit noch von Microsoft unterstützten Windows-Versionen und erlaubt die Ausführung von beliebigem Code auf entfernten Computern.

Die Schätzungen bezüglich der Anzahl der infizierten Hosts gehen auseinander. Zehn bis fünfzehn Millionen sind jedoch realistisch. Eine genaue Zahl kann nicht genannt werden, zweifellos ist die Verbreitung momentan jedoch sehr hoch.

Diese Analyse behandelt insbesondere die folgenden Fragen:

- Wie geht die Malware vor, nachdem ein Computer infiziert wurde?
- Was für Schaden wird angerichtet?
- Wie konnte beziehungsweise kann sich die Malware so schnell verbreiten?

Die nachfolgende Analyse bezieht sich auf die beiden aktuellsten Varianten Conficker.B -und C. Diese wurden um zusätzliche Verbreitungsmechanismen gegenüber Conficker.A erweitert und bringen somit neue „Features“ mit sich.

1.2 Analyisierte Datei

Die nachfolgende Tabelle beinhaltet Informationen zur analysierten Datei in gepacktem und entpacktem Zustand (Stand: 25. Februar 2009).

	Gepackt	Entpackt
Dateityp	PE (DLL)	PE (DLL)
Größe	167159 Bytes	143360 Bytes
Entrypoint	0x00019E40	0x000171CC
MD5	3aff8601a8a6fc1dcc8336ae3e971e3e	410ab4a3f49a2844013b5e2701a9683f
Virensan	38/39 ² erkannt	23/39 ³ erkannt

Tabelle 1: Dateiiinformationen

¹Im folgenden wird die Malware nur noch als „Conficker“ bezeichnet.

²<https://www.virustotal.com/analysis/ee989dd8543ed4470b875b99513eadce>

³<https://www.virustotal.com/analysis/c167e5d04085aba2332d4abafd964135>

1.3 Erstes Auftauchen

Die erste Variante der Malware – Conficker.A – wurde Microsoft erstmals am 21. November 2008 bekannt (vgl. [10]). Die ausgenützte Sicherheitslücke war zu diesem Zeitpunkt bereits fast einen Monat alt; sie wurde am 23. Oktober 2008 publiziert (vgl. [9]). Genauere Informationen zum Auftauchen von Conficker existieren nicht.

Anhand der vorliegenden Fakten kann davon ausgegangen werden, dass Conficker vermutlich zwischen Oktober und November 2008 in Umlauf gebracht wurde. Laut [10] überprüfte Conficker.A das Keymap eines Computers und sah davon ab, ukrainische Computer zu infizieren. Conficker.B und C tun dies nicht mehr. Deshalb könnte davon ausgegangen werden, dass der Wurm seinen Ursprung in der Ukraine hat.

Die folgende Aufzählung gibt einen Überblick über die wichtigsten bisherigen Ereignisse:

- 23. Oktober 2008:** Microsoft veröffentlicht den Patch für die MS08-67 Lücke (vgl. [9]).
- 21. November 2008:** Erstes Auftauchen von Conficker.A, das Microsoft bekannt wurde.
- 29. Dezember 2008:** Die zweite Variante – Conficker.B – wurde Microsoft bekannt.
- 12. Februar 2009:** Microsoft bietet \$ 250.000,- für Hinweise, die zur Fassung der Personen führen, die Conficker in Umlauf brachten [11].
- 20. Februar 2009:** Microsoft schreibt in einem Blog [13], dass eine neue Variante – Conficker.C⁴ – entdeckt wurde. Diese setzt verstärkt auf einen P2P-basierten Ansatz in Bezug auf das Nachladen von Payload.

Anfang 2009 bis heute: Zahlreiche große Netzwerke sind betroffen, darunter in Kärnten [6], [5], die deutsche Bundeswehr [7] und vermutlich das britische Militär [8].

1.4 Varianten

Wie bereits erwähnt, existieren mittlerweile drei verschiedene Varianten der Malware: Conficker.A, Conficker.B und Conficker.C. Die zweite Variante wurde Microsoft zuerst am 29. Dezember 2008 bekannt – rund einen Monat nach Auftauchen der ersten Variante Conficker.A (vgl. [10]). Der Schädling wird allerdings von Antiviren-Herstellern unterschiedlich und inkonsistent benannt, was es erschwert, die exakte Variante einer vorliegenden infizierten Datei zu bestimmen.

Die drei existierenden Varianten unterscheiden sich durch ihre Funktionalität und Verbreitungsmöglichkeiten. Die Varianten Conficker.B -und C sind auch in der Lage, sich via Netzwerkfreigaben und mobiler Datenträger zu verbreiten, wohingegen die A-Variante lediglich die Sicherheitslücke MS08-67 ausnützt (vgl. [10]).

Die neueste Variante Conficker.C reagierte auf die Bemühungen, die das Nachladen von Payload weitgehend verhinderten (siehe Abschnitt 3.4). Die Änderungen in Conficker.C sind in Abschnitt 3.4 näher beschrieben.

⁴Diese Variante wird auch Conficker.B++ genannt

2 Infektion und Weiterverbreitung

2.1 Grundlegendes

Conficker setzt den Registry-Schlüssel *TcpNumConnections* im Pfad *HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters* auf den hexadezimalen Wert `0x00FFFFFFE`. Dies ist der maximal zulässige Wert für gleichzeitig offene TCP-Verbindungen und ist standardmäßig auf diesen Wert gesetzt (vgl. [12]).

Auf diese Weise scheint der Wurm sicherzugehen, dass auch die TCP-Voraussetzungen für eine schnelle Verbreitung gegeben sind.

Zudem wird das TCP-Autotuning von Windows-Versionen mit der Major-Versionsnummer 6 (Vista, Server 2008) deaktiviert, indem der folgende Befehl ausgeführt wird:

```
netsh interface tcp set global autotuning=disabled
```

Der Wurm versucht auch, mittels einer UPNP-Nachricht ein Portforwarding zu seinem zufällig gewählten Port auf dem lokalen Gateway einzurichten (vgl. [4]).

Alle derzeit von Microsoft unterstützten Windows-Versionen sind grundsätzlich infizierbar. Zwar kann das MS08-67 Exploit in Windows Vista und Windows Server 2008 ohne vorhergehende Authentifizierung nicht angewandt werden, eine Infektion via USB-Stick oder Netzwerkfreigaben ist dennoch nicht ausgeschlossen (vgl. [9]). Betroffen sind somit die folgenden Windows-Versionen in allen Releases:

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

Conficker überprüft, ob eine Internetverbindung vorhanden ist, indem er versucht, sich zu einer der folgenden Domains zu verbinden:

- `myspace.com`
- `msn.com`
- `ebay.com`
- `cnn.com`
- `aol.com`

2.2 Die MS08-67 Lücke

Das Security Bulletin MS08-67 betrifft eine Lücke im Windows Server Service, die es einem Angreifer ermöglicht, beliebigen Code auf einem entfernten Computersystem auszuführen – bei Windows 2000, XP und Server 2003 sogar ohne vorhergehende Authentifizierung (vgl. [9]). Die Lücke befindet sich in der Bibliothek *netapi32.dll* in der Funktion `NetpwPathCanonicalize` und ist auf einen klassischen Speicherüberlauf aufgrund von mangelnder Längenüberprüfung zurückzuführen.

Diese Lücke nützt Conficker aus. Bei der A-Variante ist dies der einzige Verbreitungsweg (vgl. [10]). Conficker versucht nach der erfolgreichen Infektion eines Systems, weitere Systeme zu infizieren. Die Payload des Exploits, das an weitere Systeme geschickt wird, beinhaltet Code, der einen Callback-Mechanismus implementiert. Dieser lädt den eigentlichen Code des Wurms von dem System nach, das das Exploit ausschickte, wie in Abbildung 1 gezeigt. Dazu startet das bereits infizierte System einen primitiven Webserver auf einem beliebigen Port zwischen 1024 und 10000 (vgl. [14]). Das frisch infizierte System downloadet nun den Conficker-Code über HTTP. Dies hat für die Malware den Vorteil, dass sie nicht auf einen zentralen Server angewiesen ist, der den Conficker-Code zur Verfügung stellt.

Bevor der Webserver gestartet wird, kontaktiert Conficker noch eine der folgenden Websites, um die externe IP-Adresse des infizierten Hosts herauszufinden:

`http://www.getmyip.org`

`http://www.whatsmyipaddress.com`

`http://www.whatismyip.org`

`http://checkip.dyndns.org`

Die externe IP-Adresse wird benötigt, um anschließend den zufällig gewählten Port des Webserverns daran zu binden (vgl. [2]).

Ein Grund für die sehr schnelle Verbreitung von Conficker lag darin, dass der Patch zum Schließen der Lücke nur langsam auf betroffenen Computersystemen eingespielt wurde. Dies war und ist zweifelsohne eine starke Fahrlässigkeit der zuständigen Administratoren. Die Brisanz der Lücke wurde gemeinhin unterschätzt beziehungsweise erst gar nicht wahrgenommen. Dadurch waren bereits die Voraussetzungen gegeben, die eine ähnlich schnelle Verbreitung wie bei dem Wurm Sasser im Jahre 2004 ermöglichten.

2.3 Netzwerkfreigaben

Während die A-Variante sich auf die MS08-67 Lücke zur Verbreitung beschränkte, sind die neueren Varianten zusätzlich in der Lage, sich via Netzwerkfreigaben und mobiler Datenträger (siehe Abschnitt 2.4) zu verbreiten.

Conficker versucht sich selbst in die `ADMIN$`-Freigabe des Opferhosts zu kopieren. Dies ist standardmäßig das Verzeichnis `C:\WINDOWS`. Mithilfe der WinAPI-Funktion `NetServerEnum` suchen infizierte Computer nach weiteren Hosts. Mit den gefundenen Hosts wird wie folgt verfahren:

1. Der Wurm versucht sich mit den Credentials des gerade eingeloggtten Benutzers am

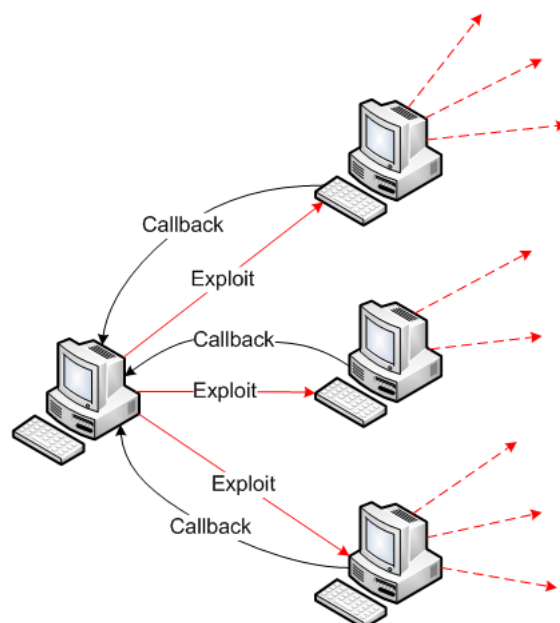


Abbildung 1: Callback-Mechanismus

entfernten Hosts zu authentifizieren (vgl. [10]).

2. Falls der vorhergehende Versuch fehlschlägt, versucht Conficker mittels der WinAPI-Funktion `NetUserEnum` eine Liste der verfügbaren Benutzer am Opferhost zu erlangen. Anschließend startet der Wurm eine Brute-Force-Attacke mit einer Wortliste von schwachen Passwörtern. Falls auf diese Weise ein Login gelingt und das geknackte Benutzerkonto Schreibrechte in der `ADMIN$`-Freigabe hat, kopiert sich der Wurm dorthin. Die Wortliste ist in Tabelle 2 abgebildet.

Falls dem Wurm auf eine der beiden beschriebenen Methoden ein Login gelingt, kopiert er sich nach `ADMIN$\System32\<zufallsfolge>.dll` und erstellt zusätzlich einen „Remote Scheduled Job“, der dazu dient, die Malware zu einem bestimmten Zeitpunkt zu starten. Der ausgeführte Befehl hat die folgende Syntax (vgl. [14]):

```
rundll32.exe <malwarename>,<zufallsfolge>
```

Wenn im lokalen Netzwerk ein Active-Directory-Dienst verwendet wird, ergibt sich ein zusätzliches Problem. Durch den Brute-Force-Angriff von Conficker kann es passieren, dass das Active Directory im Netzwerk – je nach Konfiguration – ein Benutzerkonto aufgrund von zuvielen ungültigen Login-Versuchen sperrt. Dies kann Arbeitsplatz-PCs schnell außer Betrieb bringen, da innerhalb kürzester Zeit sehr viele Konten gesperrt sein könnten und Angestellte ihre Computer nicht mehr nutzen können. Dies stellt ein Denial-of-Service-Szenario dar.

2.4 Mobile Datenträger

Schließlich nützt Conficker noch mobile Datenträger zur Verbreitung. Dazu kopiert sich der Wurm unter einem zufälligen Dateinamen auf verfügbare Datenträger. Der Pfad kann wie folgt aussehen:

```
\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\jwgkvsq.vmx
```

Zusätzlich zur DLL erstellt Conficker noch eine *autorun.inf*-Datei auf dem Datenträger. Diese ist wie folgt aufgebaut:

```
[AUTorUN]
AcTION=Open folder to view files
icon=%syStEmr0ot%\sySTEM32\shELL32.Dll,4
shellExECUte=RuNdLl32.EXE
.\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\jwgkvsq.vmx,ahaezdrn
useAuTopLAY=1
```

Die abgebildete *autorun.inf* ist „gesäubert“. Conficker schreibt viele zufällige Zeichen in die Datei, um der Signaturerkennung von Virenscannern zu entgehen.

Sobald nun ein infizierter Datenträger auf einem Computer benutzt wird, erscheint ein Fenster, wie in Abbildung 2 gezeigt. Der erste markierte Eintrag ist der vom Wurm hinzugefügte. Dieser sieht dem fünften Eintrag, der eigentlich dafür zuständig wäre, ein Explorer-Fenster zu öffnen, täuschend ähnlich.

Sobald der Benutzer darauf klickt, wird die Malware ausgeführt. Dies ist eine raffinierte und gut funktionierende Attacke, da viele Benutzer den Dialog nach dem Einstecken von Datenträgern nicht weiter beachten und die erstbeste Option anklicken. Zudem öffnet Conficker danach auch gleich ein Explorer-Fenster. Dadurch schöpfen Benutzer erst gar keinen Verdacht.

Besonders gefährlich ist diese Art der Verbreitung für Firmennetzwerke. So kann ein Firmennetzwerk zwar bereits den Patch für die MS08-67 Lücke eingespielt haben; dies nützt aber nichts, wenn Arbeitnehmer private und infizierte USB-Sticks auf einem Firmencomputer verwenden dürfen. Auf diese Weise kann der Wurm Netzwerke infizieren, die auf „herkömmlichem“ Weg nur schwer für ihn erreichbar wären.

3 Aktivität auf infizierten Hosts

3.1 Installation

Beim Einnisten in das System versucht der Wurm, sich nach *C:\WINDOWS\system32* zu kopieren. Die DLL hat einen zufälligen Dateinamen und ist versteckt. Falls dieser Versuch fehlschlägt, versucht der Wurm der Reihe nach noch die folgenden Verzeichnisse:

- *%PROGRAMFILES%\Internet Explorer*
- *%PROGRAMFILES%\Movie Maker*

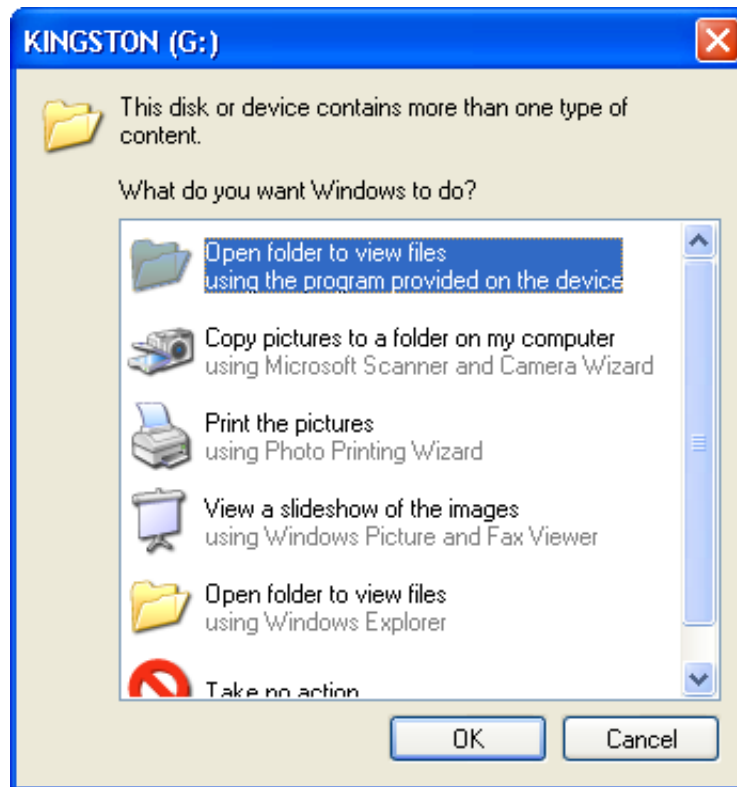


Abbildung 2: Autorun-Mechanismus

- `%APPDATA%\`
- `%TMP%\`

3.2 Verschleierung der Existenz

Conficker ergreift verschiedene Maßnahmen, die eine Entdeckung erschweren und eine Desinfektion nach Möglichkeit verhindern (vgl. [14]). Dazu gehören unter anderem folgende Registry-Schlüssel:

- Ein Registry-Schlüssel wird hinzugefügt, sodass der Benutzer keine versteckten Dateien mehr anzeigen lassen kann:
Key: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL\CheckedValue`
Value: 0
- Der Registry-Schlüssel, der für das automatische Starten von Windows Defender zuständig ist, wird gelöscht:
Key: `HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Windows Defender`

- Ein Registry-Schlüssel wird erzeugt, sodass der Wurm bei jedem Systemstart automatisch mitgestartet wird:
Key: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<zufallsfolge>`
Value: `rundll32.exe <zufallsfolge>.<zufallsfolge>`
- Der folgende Registry-Schlüssel wird gelöscht, sodass keine Warnungen des Windows Security Centers mehr angezeigt werden:
Key: `HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\ShellServiceObjects\{FD6905CE-952F-41F1-9A6F-135D9C6622CC}`

Weiters versucht der Wurm, verschiedene Dienste zu beenden, die bei seiner weiteren Verbreitung hinderlich sein könnten. Darunter fallen die folgenden (vgl. [14]):

- wscsvc (Windows Security Center Service)
- wuauclt (Windows Update Auto Update Service)
- BITS (Background Intelligence Transfer Service)
- WinDefend (Windows Defender)
- ERSvc (Error Reporting Service)
- WerSvc (Windows Error Reporting Service)

3.3 Verhinderung von Gegenmaßnahmen

Conficker installiert Hooks in DNS-Funktionen der WinAPI, wie beispielsweise `DnsQuery_A`. Diese Hooks überprüfen die DNS-Anfragen, die das System verlassen. Falls diese Strings aus Tabelle 3 enthalten, werden die DNS-Anfragen geblockt. Dadurch sollen Antiviren-Updates und Suchanfragen im Internet nach Desinfektionsmöglichkeiten verhindert werden. Abbildung 3 zeigt, dass die Webseite www.cert.at nicht aufgebaut wird, da die DNS-Anfrage nicht weitergeleitet wurde.

Abbildung 4 zeigt, wie die Funktion `Query_Main` von Conficker gehookt wurde. Der Funktionsprolog wurde entfernt und die `JMP`-Instruktion weist zur, vom Wurm implementierten Callback-Funktion, die die DNS-Anfragen überprüft.

Interessanterweise hookt Conficker auch die Funktion `NetpwPathCanonicalize`, die in der MS08-67 Lücke behandelt wird. Auf diese Weise patcht der Wurm die Lücke, sodass keine weitere Malware mehr eindringen kann. Zu beachten ist allerdings, dass dieser „Patch“ nicht persistent ist und nicht mehr greift, sobald der Hook entfernt wurde (vgl. [18]). Außerdem erlaubt dieser Hook eine Reinfektion des Hosts, da er Shellcode von Conficker erkennen kann und zulässt (vgl. [16]). Auf diese Weise können sich auch neue Varianten zukünftig schnell verbreiten, da sie bereits infizierte Hosts problemlos „updaten“ können.

Schließlich löscht Conficker noch die vom Benutzer erstellten Systemwiederherstellungspunkte (System Restore Points), damit ein einfaches Zurücksetzen des Systemzustandes nicht mehr möglich ist (vgl. [14]).

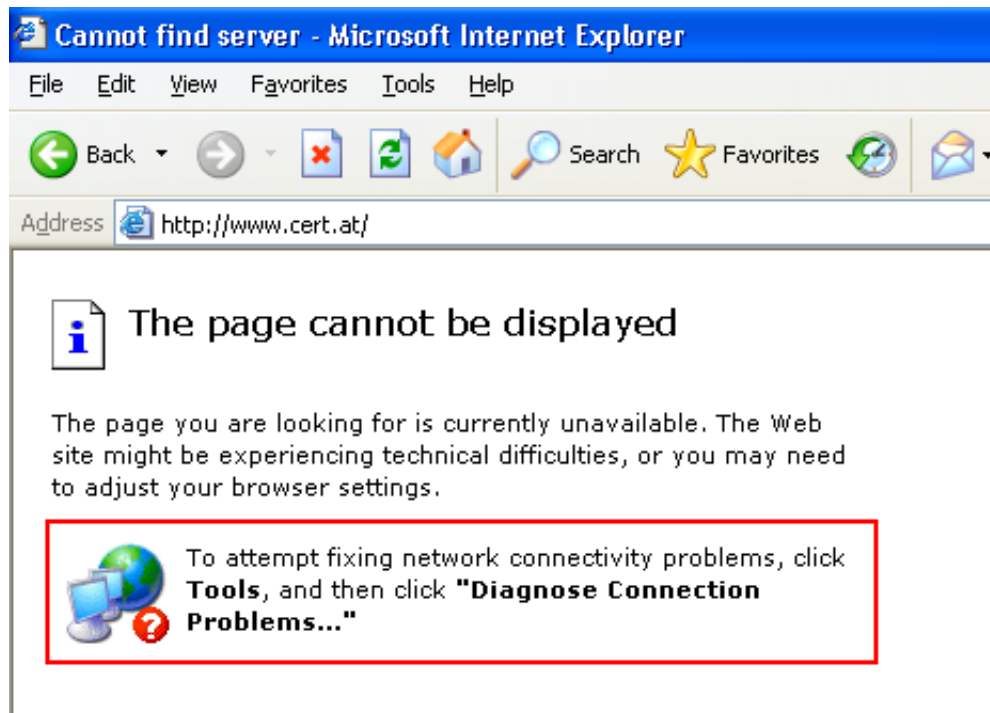


Abbildung 3: Geblockte Domains

Hooked		Initial	
dnsapi.dll:76F2498E	dnsapi_Query_Main:	dnsapi.dll:76F2498E	dnsapi_Query_Main:
dnsapi.dll:76F2498E	jmp loc_3CA04F	dnsapi.dll:76F2498E	mov edi, edi
dnsapi.dll:76F24993	;	dnsapi.dll:76F24990	push ebp
dnsapi.dll:76F24993	sub esp, 1Ch	dnsapi.dll:76F24991	mov ebp, esp
dnsapi.dll:76F24996	push ebx	dnsapi.dll:76F24993	sub esp, 1Ch
dnsapi.dll:76F24997	push esi	dnsapi.dll:76F24996	push ebx
dnsapi.dll:76F24998	mov esi, [ebp+8]	dnsapi.dll:76F24997	push esi
dnsapi.dll:76F2499B	mov edx, [esi+10h]	dnsapi.dll:76F24998	mov esi, [ebp+8]
dnsapi.dll:76F2499E	push edi	dnsapi.dll:76F2499B	mov edx, [esi+10h]
dnsapi.dll:76F2499F	xor eax, eax	dnsapi.dll:76F2499E	push edi
dnsapi.dll:76F249A1	push 2	dnsapi.dll:76F2499F	xor eax, eax
dnsapi.dll:76F249A3	xor ecx, ecx	dnsapi.dll:76F249A1	push 2
dnsapi.dll:76F249A5	inc ecx	dnsapi.dll:76F249A3	xor ecx, ecx
dnsapi.dll:76F249A6	push ecx	dnsapi.dll:76F249A5	inc ecx
dnsapi.dll:76F249A7	push eax	dnsapi.dll:76F249A6	push ecx
dnsapi.dll:76F249A8	push dword ptr [esi]	dnsapi.dll:76F249A7	push eax
dnsapi.dll:76F249AA	mov [ebp-14h], eax	dnsapi.dll:76F249A8	push dword ptr [esi]
dnsapi.dll:76F249AD	mov [esi+3Ch], eax	dnsapi.dll:76F249AA	mov [ebp-14h], eax

Abbildung 4: Hooking der DNS-API

Die Analyse des Wurms wurde durch „Packing“ der ausführbaren Datei erschwert. Diese wurde zweifach mithilfe des Packers UPX⁵ gepackt. Die ausführbare Datei wurde allerdings noch manuell verändert, sodass sie nicht mehr automatisch mit UPX entpackt werden konnte.

3.4 Nachladen von Payload

Conficker selbst beinhaltet keinen schadhafte Code, um beispielsweise Kreditkartendaten auszuspähen. Der Conficker-Code ist alleine für die Verbreitung zuständig und beinhaltet Mechanismen, die zusätzliche Payload nachladen können.

Um eine Fernsteuerung zu ermöglichen, kontaktieren infizierte Computer ab dem 1. Januar 2009 (Conficker.B) eine bestimmte Reihe an Domains⁶ und versuchen eine Datei zu downloaden. Diese Domains werden zufällig generiert. Initialisiert wird der Zufallszahlengenerator mit der aktuellen Zeit. Die verwendeten TLDs sind *.biz*, *.info*, *.org*, *.net*, *.ws*, *.cn*, *.cc* und *.com*. Tabelle 4 zeigt einige der verwendeten Domains.

Der Wurm bettet die zufällig generierten Domains in die folgende URL ein und schickt dafür HTTP GET-Anfragen ab:

`http://<zufallsdomain>/search?q=<infectioncount>`. Der Parameter `<infectioncount>` gibt die Anzahl der vom Wurm bereits infizierten Hosts an.

Dieses Konzept verlangt es, dass die Autoren von Conficker rechtzeitig die jeweiligen Domains registrieren und Malware auf den HTTP-Servern platzieren, die anschließend von den infizierten Hosts downgeloadet, authentifiziert und ausgeführt wird.

Die Dateien, die der Wurm auf diese Weise downloadet, enthalten eine digitale Signatur und werden mittels Public-Key-Kryptographie authentifiziert. Auf diese Weise wollten die Autoren von Conficker verhindern, dass andere Kriminelle im voraus Domains für Conficker registrieren und ihre eigene Malware damit verbreiten (vgl. [16]).

Der Algorithmus zur Generierung der Zufalls-Domains ist rekonstruiert worden. Die Domains, die der Wurm in Zukunft kontaktieren wird sind außerdem schon von einer Gruppe von Sicherheitsexperten registriert worden, sodass sie nicht mehr zur Verbreitung von zusätzlicher Malware verwendet werden können (vgl. [15]). So sieht der Registrierungseintrag der Domain „pwulrrog.org“ wie folgt aus:

```
Domain ID:D155329089-LROR
Domain Name:PWULRROG.ORG
Created On:10-Feb-2009 23:47:07 UTC
Last Updated On:11-Feb-2009 00:18:18 UTC
Expiration Date:10-Feb-2010 23:47:07 UTC
Sponsoring Registrar:PIR Special Projects (R1776-LROR)
Status:TRANSFER PROHIBITED
Registrant ID:Special-001
Registrant Name:Conficker Cabal
Registrant Organization:Microsoft
```

⁵<http://upx.sourceforge.net>

⁶Diese werden auch „Rendez-Vous Points“ genannt

```
Registrant Street1:One Microsoft Way  
[...]
```

Auch das OpenDNS-Projekt stellt mittlerweile eine Möglichkeit bereit, die die von Conficker automatisch generierten Domains erkennen und blocken kann (vgl. [17]).

Weil das Nachladen von Payload durch die oben genannten Maßnahmen sehr erschwert wurde, reagierten die Autoren von Conficker mit der neuen C-Variante. Diese verfügt über zwei nennenswerte Änderungen:

- **Reinfektion:** Der Hook der Funktion `NetpwPathCanonicalize` wurde dahingehend erweitert, dass nun ein Angreifer für die Callback-Infektionsmethode eine beliebige URL einer signierten EXE-Datei angeben kann. Die downgeladete Datei wird – sofern die Überprüfung der Signatur erfolgreich war – direkt ausgeführt. Dadurch ist es möglich, den MS08-67 Exploit zu nutzen, um beliebige Payload an bereits infizierte Hosts zu schicken, die ausgeführt wird (vgl. [16]).
- **Named Pipes:** Der Wurm erstellt eine Named Pipe, über die URLs mit entfernten Hosts ausgetauscht werden können. Diese URLs können wiederum auf signierte Payload zeigen, die direkt ausgeführt wird, nachdem die Signatur überprüft wurde. Diese Named Pipe wird bei Windows-Versionen der Major-Versionsnummer 5 (Windows 2000, XP, Server 2003) erstellt.

Beide neu hinzugefügte Verbreitungswege verfolgen einen P2P-Ansatz, während das vorhergehende Modell der zufällig kontaktierten Domains Client-to-Server basiert war. Dieser Ansatz ist aufgrund der Flexibilität und dezentralen Funktionsweise nicht mehr so einfach auszuschalten wie das ursprüngliche Client-to-Server basierte Modell der zufälligen Domains.

Bis heute wurde noch nicht beobachtet, ob und was Conficker für Payload nachlädt. Zweifellos funktionieren die Routinen, die Payload nachladen sollen, ob sie auch schon in Verwendung sind, ist jedoch nicht bekannt (vgl. [3]).

4 Abwehr und Prävention

4.1 Rechtzeitiges Patchen

Wie bereits erwähnt, wurde der MS08-67 Patch zu langsam eingespielt. Dies trifft auf Privatanwender genauso wie auf Firmennetzwerke zu. Zwar verfügt der Wurm auch über andere Verbreitungsarten, die Geschwindigkeit der Ausbreitung hätte durch schnelles Einspielen des Patches allerdings wesentlich eingedämmt werden können.

Unternehmen, die davon betroffen waren, sollten eine Patchmanagement-Strategie entwickeln. Zudem sollte auch die jeweilige Firewall-Policy überdacht werden. Port 139 (NetBIOS) und 445 (SMB) sollten vom Internet aus nicht erreichbar sein und können durch Paketfiltering-Regeln verworfen werden.

4.2 Sicherheitspolicies

Mobile Datenträger erwiesen sich in einigen Netzwerken als ebenso großes Problem. Anwender konnten problemlos USB-Sticks in ihren Computern verwenden und schleusten so Conficker in das Netzwerk ein. Auf diese Weise konnte Conficker problemlos Netzwerke erschließen, die sogar gegen die MS08-67 Lücke gepatcht waren.

In diesem Fall empfiehlt es sich dringend, Gruppenrichtlinien zu erstellen, die Anwendern verbietet, USB-Sticks und andere mobile Datenträger zu verwenden. Von Conficker abgesehen wird auch andere Malware maßgeblich durch mobile Datenträger verbreitet.

4.3 Starke Passwörter

Schließlich waren an der schnellen Verbreitung Confickers noch schwache Passwörter schuld. Dieses Thema ist jedoch alles andere als neu und sollte jedem Administrator bekannt sein.

5 Fazit

Conficker nützte ursprünglich eine sehr kritische Lücke in Windows und konnte sich überaus schnell verbreiten, da nach wie vor viele Computer ungepatcht sind. Der Wurm ist mittlerweile fast vier Monate in Umlauf und immer noch eine große Bedrohung – nicht zuletzt deswegen, weil noch keine Hinweise auf nachgeladene Payload existieren. Eine kleine Unachtsamkeit mit einem infizierten USB-Stick genügt, um den Schädling in große Netzwerke einzuschleusen.

Betroffene Nutzer wissen vermutlich oft gar nicht, dass ihr Computer infiziert ist, da Conficker sehr unauffällig agiert. Aus der Sicht eines wenig versierten Anwenders ändert sich schlicht nichts am Verhalten eines infizierten Hosts.

Der größte Schaden, den Conficker bislang anrichtete bestand darin, dass aufgrund der Brute-Force-Attacken Benutzerkonten von Active-Directory-Diensten kurzzeitig gesperrt wurden. Ansonsten gibt es, wie bereits erwähnt, noch keine Indizien dafür, dass beispielsweise nachgeladene Keylogger auf infizierten Computern schon Kreditkartendaten abgreifen. Die eigentlichen Schadroutinen wurden offenbar noch nicht genutzt, wenngleich sie jederzeit aktiv sind und auch funktionieren.

Es gibt einige Bestrebungen, die Verbreitung von Conficker einzudämmen. So wurde der Algorithmus zur Generierung von Zufallsdomains offengelegt und all diese Domains stehen mittlerweile unter Beobachtung oder sind bereits registriert. Auf diese Weise werden die Autoren keine Payload mehr nachladen können. Dies ist aufgrund des neuen Ansatzes von Conficker.C auch nicht mehr nötig, da dieser flexibler agiert und nicht mehr auf zentrale Downloadpunkte angewiesen ist.

Noch ist nicht klar, wer hinter Conficker steckt. Zweifellos handelt es sich um organisierte Kriminelle mit hohem Wissen und Erfahrung. Symantec vermutet hinter dem Wurm eine bekannte Malware-Gruppe [1]. Nähere Informationen dazu sind jedoch nicht bekannt.

6 Anhang

0000	33333333	9999999	cookie	nimda	secret
00000	4321	99999999	customer	nobody	secure
0000000	4444	Admin	database	nopass	security
00000000	44444	Internet	default	nopassword	server
0987654321	444444	Login	desktop	nothing	shadow
1111	4444444	Password	domain	office	share
11111	44444444	a1b2c3	example	oracle	student
111111	54321	aaaa	exchange	owner	super
1111111	5555	aaaaa	explorer	pass	superuser
11111111	55555	abc123	file	pass1	supervisor
123123	555555	academia	files	pass12	system
12321	5555555	access	foobar	pass123	temp
123321	55555555	account	foofoo	passwd	temp123
1234	654321	admin	forever	password	temporary
12345	6666	admin1	freedom	password1	temptemp
123456	66666	admin12	fuck	password12	test
1234567	666666	admin123	games	password123	test123
12345678	6666666	adminadmin	home	private	testtest
123456789	66666666	administrator	home123	public	unknown
1234567890	7654321	anything	ihavenopass	pw123	windows
1234abcd	7777	asdds	internet	q1w2e3	work
1234qwer	77777	asdfgh	intranet	qazwsx	work123
123abc	777777	asdsa	killer	qazwsxedc	xxxx
123asd	7777777	asdzc	letitbe	qqqq	xxxxx
123qwe	77777777	backup	letmein	qqqqq	zxcxzx
1q2w3e	87654321	boss123	login	qwe123	zxcvbn
2222	8888	business	lotus	qweasd	zxcvbn
22222	88888	campus	love123	qweasdzxc	zxcxz
222222	888888	changeme	manager	qweewq	zzzz
2222222	8888888	cluster	market	qwerty	zzzzz
22222222	88888888	codename	money	qwewq	
3333	987654321	codeword	monitor	root	
33333	9999	coffee	mypass	root123	
333333	99999	computer	mypassword	rootroot	
3333333	999999	controller	mypc123	sample	

Tabelle 2: Wortliste

ahnlab	computerassociates	gdata	networkassociates	sophos
arcabit	cpsecure	grisoft	nod32	spamhaus
avast	defender	hacksoft	norman	spyware
avg.	drweb	hauri	norton	sunbelt
avira	emsisoft	ikarus	panda	symantec
avp.	esafe	jotti	pctools	threatexpert
bit9.	eset	k7computing	prevx	trendmicro
castlecops	etrust	kaspersky	quickheal	vet.
centralcommand	ewido	malware	rising	virus
cert.	f-prot	mcafee	rootkit	wilderssecurity
clamav	f-secure	microsoft	sans.	windowsupdate
comodo	fortinet	nai.	securecomputing	

Tabelle 3: DNS-Strings

dozjritemv.info	dyjsialozl.ws	eaieijqcqlv.org	eewxsvtkyn.net
eidqdorgmbr.net	eiqzexpacyb.cn	ejdmzbzzaos.biz	ejmxd.com
ejzrcqqw.net	ekusgwp.cc	eprhdsudnnh.biz	evmwwgi.ws
falru.net	fctkztzhyr.org	fdkjan.net	fhfntt.org
fhspuip.biz	fjpszgrf.net	fkzdr.cn	ftjggny.com
fuiumrawg.info	ghdkt.cn	glbmkbmdax.biz	gmhkdp.org
gocpopuklm.org	grwemw.biz	gtzaick.cc	gxzlgsoa.info
gypqfjho.info	hduyjkrouop.info	hfgxlzjbfka.biz	hkgzoi.com

Tabelle 4: Domains

Literatur

- [1] CHIEN, E.: *Downadup: Peer-to-Peer Payload Distribution*, 2009. URL: https://forums.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/227, (Abruf: 24. 02. 2009).
- [2] F-SECURE CORPORATION: *F-Secure Malware Information Pages: Worm:W32/Downadup.AL*, 2009. URL: http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml, (Abruf: 16. 02. 2009).
- [3] FLORIO, E.: *Downadup—Advanced Crypto Protection*, 2009. URL: <https://forums.symantec.com/t5/Malicious-Code/Downadup-Advanced-Crypto-Protection/ba-p/391311#A246>, (Abruf: 24. 02. 2009).
- [4] FORTINET INC.: *In-Depth Analysis*, 2009. URL: <http://www.fortiguardcenter.com/virusency/W32/Conficker.B!worm>, (Abruf: 21. 02. 2009).
- [5] HEISE ZEITSCHRIFTEN VERLAG: *Conficker in Kärnten: Nach der Landesregierung nun die Spitäler*, 2009. URL: <http://www.heise.de/security/Conficker-in-Kaernten-Nach-der-Landesregierung-nun-die-Spitaeler--/news/meldung/121570>, (Abruf: 15. 02. 2009).
- [6] HEISE ZEITSCHRIFTEN VERLAG: *Conficker schlägt bei Kärntner Regierung zu*, 2009. URL: <http://www.heise.de/security/Conficker-schlaegt-bei-Kaerntner-Regierung-zu--/news/meldung/121387>, (Abruf: 15. 02. 2009).
- [7] HEISE ZEITSCHRIFTEN VERLAG: *Hunderte Bundeswehr-Rechner von Conficker befallen*, 2009. URL: <http://www.heise.de/newsticker/Hunderte-Bundeswehr-Rechner-von-Conficker-befallen--/meldung/132555>, (Abruf: 15. 02. 2009).
- [8] HEISE ZEITSCHRIFTEN VERLAG: *Wurm dringt in Systeme der britischen Armee ein*, 2009. URL: <http://www.heise.de/security/Wurm-dringt-in-Systeme-der-britischen-Armee-ein--/news/meldung/122112>, (Abruf: 15. 02. 2009).
- [9] MICROSOFT CORPORATION: *Microsoft Security Bulletin MS08-067 – Critical*, 2008. URL: <http://www.microsoft.com/technet/security/Bulletin/MS08-067.aspx>, (Abruf: 15. 02. 2009).
- [10] MICROSOFT CORPORATION: *Centralized Information About The Conficker Worm*, 2009. URL: <http://blogs.technet.com/mmcp/archive/2009/01/22/centralized-information-about-the-conficker-worm.aspx>, (Abruf: 15. 02. 2009).

-
- [11] MICROSOFT CORPORATION: *Microsoft Collaborates With Industry to Disrupt Conficker Worm*, 2009. URL: <http://www.microsoft.com/Presspass/press/2009/feb09/02-12ConfickerPR.aspx>, (Abruf: 16. 02. 2009).
- [12] MICROSOFT CORPORATION: *TcpNumConnections: Core Services*, 2009. URL: <http://technet.microsoft.com/en-us/library/cc758980.aspx>, (Abruf: 17. 02. 2009).
- [13] MICROSOFT CORPORATION: *Updated Conficker Functionality*, 2009. URL: <http://blogs.technet.com/mmpc/archive/2009/02/20/updated-conficker-functionality.aspx>, (Abruf: 22. 02. 2009).
- [14] MICROSOFT CORPORATION: *Worm:Win32/Conficker.B*, 2009. URL: <http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm:Win32/Conficker.B>, (Abruf: 16. 02. 2009).
- [15] NAZARIO, J.: *The Conficker Cabal Announced*, 2009. URL: <http://asert.arbornetworks.com/2009/02/the-conficker-cabal-announced/>, (Abruf: 22. 02. 2009).
- [16] PHILLIP PORRAS, HASSEN SAIDI, V. Y.: *An Analysis of Conficker's Logic and Rendezvous Points*, 2009. URL: <http://mtc.sri.com/Conficker/>, (Abruf: 22. 02. 2009).
- [17] ULEVITCH, D.: *Stats are back; and we're blocking Conficker*, 2009. URL: <http://blog.opendns.com/2009/02/09/stats-are-back-and-conficker/>, (Abruf: 17. 02. 2009).
- [18] ZDRNJA, B.: *Some tricks from Conficker's bag*, 2009. URL: <http://isc.sans.org/diary.html?storyid=5830>, (Abruf: 17. 02. 2009).